ALGEBRA 1

nhsm student

Chapter 01: Mathematical logic ans sets

1 Mathematical logic :

1.1 Generalities :

statement : a declarative sentence that is either true or false (but not both) .
we have some types of statements such as : axiom ; definition ; conjecture ; theorem .
as for theorems we have : proposition ; lemma ; corollary .

1.2 The truth table :

the truth table indicates all possible values (the truth values) of a given statement .
the truth value of a statement can be either ″1/T″ which indicates that it is true or ″0/F″ which indicates that it is false.

statement
1
0

Proof :

it is an argument that shows the truth of a mathematical statement using axioms , definitions and previously proven theorems .
Note : the argument must be clear and without any gaps or errors .

1.3 The logical connectives :

Negation : ″not″

$\neg P$ is the negation of P which have the opposite truth values of P .

Conjunction : ″and″

$P \wedge Q$ is the conjunction of P and Q is true only when both P and Q are true .

Disjunction : ″or″

$P \vee Q$ is the disjunction of P and Q it is false only when both P and Q are false .

implication : ″conditional statement″

$P \Rightarrow Q$ ″P implies Q″ or ″if P then Q″ which is false only when P is true and Q is false

Equivalence : ″bi-conditional statement″

$P \Leftrightarrow Q$ ″P if and only if Q″ or ″P is equivalent to Q″ it is only true when both P and Q have the same truth value

P	Q	$\neg P$	$P \wedge Q$	$P \vee Q$	$P \Rightarrow Q$	$P \Leftrightarrow Q$
1	1	0	1	1	1	1
1	0	0	0	1	0	0
0	1	1	0	1	1	0
0	0	1	0	0	1	1

Theorem : Let P and Q be two statements :

1. $(P \Rightarrow Q) \Leftrightarrow (\neg P \vee Q)$
2. $(P \Leftrightarrow Q) \Leftrightarrow [(P \Rightarrow Q) \wedge (Q \Rightarrow P)]$
3. $\neg(P \Leftrightarrow Q) \Leftrightarrow (\neg P \Leftrightarrow Q)$

Tautologies and contradiction :

Tautologies ″T″ : is a compound statement that is always true

Contradiction ″C″ : is a compound statement that is always false

1.4 Laws of logic :

Given some statements ″ P , Q , R ″ ; a tautology ″T″ ; a contradiction ″C″
the following statements hold :

1. The identity laws : $(P \wedge T) \Leftrightarrow (P \vee C) \Leftrightarrow P$
2. Domination laws : $(P \wedge C) \Leftrightarrow C$; $(P \vee T) \Leftrightarrow T$
3. Indenpotent laws : $(P \vee P) \Leftrightarrow P$; $(P \wedge P) \Leftrightarrow P$
4. Double negation : $(\neg\neg P) \Leftrightarrow P$
5. Negation laws : $(P \wedge \neg P) \Leftrightarrow C$; $(P \vee \neg P) \Leftrightarrow T$
6. Associative laws :$P \wedge (Q \wedge R) \Leftrightarrow (P \wedge Q) \vee R$; $P \vee (Q \vee R) \Leftrightarrow (P \vee Q) \vee R$
7. Distributive laws : $P \wedge (Q \vee R) \Leftrightarrow [(P \wedge Q) \vee (P \wedge R)]$; $P \vee (Q \wedge R) \Leftrightarrow [(P \vee Q) \wedge (P \vee R)]$
8. DeMorgan laws : $\neg(P \wedge Q) \Leftrightarrow (\neg P \vee \neg Q)$; $\neg(P \vee Q) \Leftrightarrow (\neg P \wedge \neg Q)$
9. Commutative laws : $(P \wedge Q) \Leftrightarrow (Q \wedge P)$; $(P \vee Q) \Leftrightarrow (Q \vee P)$
10. Absltion laws : $[P \wedge (P \vee Q)] \Leftrightarrow P$; $[P \vee (P \wedge Q)] \Leftrightarrow P$

1.5 The quantifiers :

Predicate : is a phrase written with variables that for every value of the variables it is a statement , we use quantifiers to precise the statement we want to prove .

- **Universal quantifier : "$\forall$ / for all "**
  For all x of D (for every x of D) P(x) is satisfied "$\forall x \in D; P(x)$ "
- **Existential quantifier : "$\exists$ / there exist "**
  There exist x of D (for some x of D) P(x) is satisfied "$\exists x \in D; P(x)$ "

Remark : let D= $\{x_1, x_2, x_3, ..., x_n\}$
$\forall x \in D; P(x) \Leftrightarrow P(x_1) \wedge P(x_2) \wedge P(x_3) \wedge \ldots \wedge P(x_n)$
$\exists x \in D; P(x) \Leftrightarrow P(x_1) \vee P(x_2) \vee P(x_3) \vee \ldots \vee P(x_n)$

- **Negation quantified expressions :**
  the negation of $\forall x \in D; P(x)$ is $\exists x \in D; \neg P(x)$
  the negation of $\exists x \in D; P(x)$ is $\forall x \in D; \neg P(x)$

Remarks :
The statement $\forall x \in D, \forall y \in D; P(x, y)$ is equivalent to $\forall y \in D, \forall x \in D; P(x, y)$ and the statement $\exists x \in D, \exists y \in D; P(x, y)$ is equivalent to $\exists x \in D, \exists y \in D; P(x, y)$
The statement $\forall x \in D, \exists y \in D; P(x, y)$ isn't the same as $\exists y \in D, \forall x \in D; P(x, y)$
The statement $\forall x \in D; P(x) or Q(x)$ isn't the same as $(\forall x \in D; P(x)) or (\forall x \in D; Q(x))$
The statement $\exists x \in D; P(x) and Q(x)$ isn't the same as $(\exists x \in D; P(x)) and (\exists x \in D; Q(x))$

1.6 Methods of proof :

- **Direct proof :** is to show that from $P \Rightarrow Q$ we assume that P is true and we show that Q is true using axioms and proven theorems and definitions .
- **Proof by counter example :** we give an example that doesn't satisfy the statement
- **Proof by contraposition (contrapositive) :** using the fact that $(P \Rightarrow Q) \Leftrightarrow (\neg P \Rightarrow \neg Q)$
- **Proof by contradiction :** to show that P is true we suppose that $\neg P$ is true and we try to prove it and we deduce that $\neg P$ is false and that means that P is true
- **Proof by cases :** sometimes the hypothesis of a statement can be broken down into simple cases that are simple to prove . This proof is based on the equivalence $[(P1 \wedge P2 \wedge P3 \wedge ... \wedge Pn) \Rightarrow Q] \Leftrightarrow [(P1 \Rightarrow Q) \wedge (P2 \Rightarrow Q) \wedge (P3 \Rightarrow Q) \wedge ... \wedge (Pn \Rightarrow Q)]$
- **Proof by induction :** is a technique used to show that a certain type of mathematical statements hold , it is based on proving that a statement is true for all $n \geq n_0$:
  i) prove the base case : $P(n_0)$ is true ; ii) suppose that P(n) is true ; iii) try to prove P(n+1)
  at the end we conclude that P(n) is true $\forall n \geq n_0$
  Strong induction : suppose P(n) is true $\forall n \geq n_0$, if P(k) is true $\forall n \geq k \geq n_0$, then P(n) is true $\forall n \geq n_0$.

2 Sets :

2.1 Generalities :

- **Set :** is a collection of elements or numbers .
- **Empty set " $\emptyset; \{\}$ ":** is a collection that contains no element .
- **Finite set :** is a set that contains a finite number of elements else it is **infinite**.
- **Cardinality / size of a set "S" "** $|S|; Card(S)$ **" :** is the number of elements of a set ($|S| \in \mathbb{N}_0$).
- if x belongs to S then we write $x \in S$ otherwise $x \notin S$ (doesn't belong).
- we represent a set by :
  listing : enumerating the elements of the set .
  Defining by property : using the set *builder notation* $S = \{x \mid x\ verify\ a\ property\}$

2.2 Inclusion and Equality :

$A \subset B$ "A is **included** in B "/"B **includes** A" : $\forall a \in A\ ;\ a \in B$.
AB "A **isn't included** in B" : $\exists a \in A\ ;\ a \notin B$.
Equality of two stes : if $A \subset B$ and $B \subset A$ then A = B "A is equal to B ".

Theorem 1 *let A and B be two finite sets :*

- $B \subset A \Rightarrow |A| \geq |B|$
- $\emptyset \subset A$
- $A \subset A$
- $[(A \subset B) \wedge (B \subset C)] \Rightarrow (A \subset C)$

Power set : S is a set , P(S) is the set of all subsets of S and it is caller the set of parts also.

$$P(S) = \{X | X \subset S\}$$

Note : $X \in P(E) \Rightarrow X \subset E\ ;\ X = \{x\}, X \in P(E) \Rightarrow x \in E\ ;\ X \subset E, X \cap E = X, X \cup E = E\ ;$
$S = \emptyset, P(S) = \{\emptyset\}, P(P(S)) = \{\emptyset, \{\emptyset\}\}$
S is a finite set $\Rightarrow |P(S)| = 2^{|S|}$.

2.3 Intersection and Union :

Intersection of two sets : $(A, B) \in P(S)$

$A \cap B = \{x \in S | x \in A\ and\ x \in B\}\ ;\ A \cap B \subset S$
if $A \cap B = \emptyset$ then A and B are **disjoint**.

Union of two sets : $(A, B) \in P(S)$

$A \cup B = \{x \in S | x \in A or x \in B\}$; $A \cup B \subset S$

Note :

- $A \cap \emptyset = \emptyset \ \wedge \ A \cup \emptyset = A$
- $(A \cap B) \subset A \ \wedge \ (A \cap B) \subset B$; $A \subset (A \cup B) \ \wedge \ B \subset (A \cup B)$
- $A \cup B = A \Leftrightarrow B \subset A$

2.4 Complement of a set : $A \in P(S)$

$\overline{A} = C_S(A) = \{x \in S | x \notin A\}$ is the complement of A .

Theorem 2 $(A, B \in P(S))$

- $C_S(C_S(A)) \ = \ A$
- $A \subset B \Leftrightarrow C_S(B) \subset C_S(A)$
- $C_S(A \cup B) \ = \ C_S(A) \cap C_S(B)$; $C_S(A \cap B) = C_S(A) \cup C_S(B)$

2.5 Difference of two sets : $(A, B) \in P(S)$

The difference : $A - B \ = \ A \setminus B = \{x \in A | x \notin B\}$
The symmetric difference : $A \triangle B \ = \ (A \cup B) \setminus (A \cap B)$

2.6 The Cartesian product : ($X, Y \neq \emptyset$)

$X \times Y = \{(x, y) | x \in X \ , \ y \in Y\}$ is the cartesian product of X and Y .
Remark :

- if X=Y ,then $X \times X = X^2$; In general : if $X_1, X_2, ...X_n \neq \emptyset$; $(for \ n \geq 2)$
  $X_1 \times X_2 \times ... \times X_n = \{(x_1, x_2, ..., x_n) | x_i \in X_i \ , \ i = \overline{(1, n)}\}$
  $if X_1 = X_2 = ... = X_n = X \ then \ X_1 \times X_2 \times ... \times X_n = X^n$.
- in general $(X \times Y) \neq (Y \times X)$; $X = \emptyset$ or $Y = \emptyset$ iff $X \times Y = \emptyset$
- $|X \times Y| \ = \ |X| \ . \ |Y|$

2.7 Indesced sets : $i \in I \subset \mathbb{N}_0$

$\underset{i \in I}{\cup} A_i = \{x \mid x \in A_i$ for at least one of $A_i\}$.
$\underset{i \in I}{\cap} A_i = \{x | x \in A_i, \forall i \in I\}$.
Partition : let $i, j \in I$, (Ai) is a partiition of A $\Leftrightarrow A_i \cap A_j = \emptyset$, $\underset{i \in I}{\cup} A_i = A$.

Chapter 02: Maps and Binary relations

3 Maps :

Generalities :

- A well defined Map from the **Domain** A to the **Codomain** B : $\forall x \in A, \exists! y \in B; f(x) = y$
- we denote a map by :

$$f : A \longrightarrow B$$
$$x \mapsto f(x) = y$$

- **Graph of a map :** is the set (x"pre-image" ; f(x)"image") that uniquely represents the map .
- **Equality of two maps :** $f = g \Leftrightarrow (A = A') \wedge (B = B') \wedge (f(x) = g(x))$

3.1 Some useful maps : $(A, B \neq \emptyset), (A' \neq \emptyset / A' \subset A)$

- **Constant map :**

$$f : A \longrightarrow B$$
$$x \mapsto c$$

- **Identity map (Id) :**

$$Id_A : A \longrightarrow A$$
$$x \mapsto x$$

- **Indicator map:** $X_A(x) = \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{if } x \notin A \end{cases}$; $X_A(x) : A \longrightarrow \{1, 0\}$.
- **Projection maps :**

$$Pr_A : A \times B \longrightarrow A$$
$$(x, y) \mapsto x$$

- **Inclusion maps :** $i_{A'} = Id_{/A'}$

$$i_{A'} : A' \longrightarrow A$$
$$x \mapsto x$$

3.2 Restriction of a map : $f : A \longrightarrow B$, $\emptyset \neq A' \subset A$

The restriction of f to A

$$f_{/A'} : A' \longrightarrow B$$
$$x \mapsto f(x)$$

3.3 Corestriction of a map : $f : A \longrightarrow B$, $\emptyset \neq B' \subset B$, $\forall x \in A, f(x) \in B'$

The corestriction of f to B

$$f^{/B'} : A \longrightarrow B'$$
$$x \mapsto f(x)$$

3.4 The composition of two maps : $f : A \longrightarrow B, g : B \longrightarrow C$

g round f or f composed with g , $(gof)(x) = g(f(x))$:

$$gof : A \longrightarrow C$$
$$x \mapsto g(f(x))$$

"In general $(fog \neq gof)$"

$$f : A \longrightarrow B \text{ , } g : B \longrightarrow C \text{ , } h : C \longrightarrow D \text{ ; } h \; o \; (\; g \; o \; f \;) : A \longrightarrow D = (\; h \; o \; g \;) \; o \; f : A \longrightarrow D$$

$$\forall f : A \longrightarrow B, f \; o \; Id_A = Id_B \; o \; f = f$$

3.5 Injective maps :

$$\forall x_1, x_2 \in X, f(x_1) = f(x_2) \Rightarrow x_1 = x_2 \;\; or \;\; \forall x_1, x_2 \in X, f(x_1) \neq f(x_2) \Rightarrow x_1 \neq x_2$$

"It's negation is : " $\exists x_1, x_2 \in X, f(x_1) = f(x_2) \wedge x_1 \neq x_2$

The equation $\begin{cases} y = f(x) \\ x \in X \end{cases}$ has at most one solution $\forall y \in Y$

Note : If f is injective and g is injective then fog is injective

3.6 Surjective maps :

$$\forall y \in Y, \exists x \in X, f(x) = y$$

"It's negation is : " $\exists y \in Y, \forall x \in X; f(x) \neq y$

The equation $\begin{cases} y = f(x) \\ x \in X \end{cases}$ has at least one solution $\forall y \in Y$

Note : If f is surjective and g is surjective then fog is surjective

3.7 Bijective maps :

$$\forall y \in Y, \exists! x \in X; f(x) = y$$

The equation $\begin{cases} y = f(x) \\ x \in X \end{cases}$ has exactly one solution $\forall y \in Y$

Note 1 : If f is injective and it is surjective then it is bijective ,to prove that f isn't bijective we only need to prove that it isn't surjective or it isn't injective .

Note 2 : If f is bijective and g is bijective then fog is bijective

3.8 The inverse of a bijective map : $\forall y \in B, \exists! x \in A; f(x) = y$

$$f : A \longrightarrow B$$
$$x \mapsto f(x) = y$$
$$f^{-1} : B \longrightarrow A$$
$$y \mapsto f^{-1}(y) = x$$

Notes :

- $(f^{-1})^{-1} = f$
- if f is bijective then f^{-1} exists and is unique
- $fof^{-1} = Id_B \wedge f^{-1}of = Id_A$

Two sets with the same size :

if there is a bijection $f : A \longrightarrow B$ then A and B have the same **Cardinality** .
$(A \approx B \Rightarrow B \approx A)$; $(A \approx B \wedge B \approx C \Rightarrow A \approx C)$

Countable and uncountable sets :

A is countably infinite if $A \approx \mathbb{N}$.
A is countable if either A is countably infinite or if A is finite .
If A isn't countable we say A is uncountable (infinite).

3.9 Image and Pre-image of a set by a map :

Image of a set by a map : $A \subset X; f : X \longrightarrow Y$
$f(A) = \{f(x) \in Y | x \in A\}$
Pre-image of a set by a map : $B \subset Y; f : X \longrightarrow Y$
$f^{-1}(B) = \{x \in X | f(x) \in B\}$

4 Binary relations :

Let R be a binary relation such that if two elements x and y of A are related by R we type xRy

4.1 Some Properties for Binary relations :

- R is **Reflexive :** $\forall x \in A \ ; \ xRx$.
- R is **Symmetric :** $\forall x, y \in A \ ; \ AxRy \Rightarrow yRx$.
- R is **Transitive :** $\forall x, y, z \in A \ ; \ xRy \wedge yRz \Rightarrow xRz$.
- R is **Anti-symmetric :** $\forall x, y \in A \ ; \ (\ xRy \ ) \wedge (\ yRx \ ) \Rightarrow x = y$.

4.2 Types of binary relations :

4.2.1 Equivalence relations :

- R must be reflexive , symmetric and transitive
- $\overline{a}$ is the **representative** of the equivalence class
- The quotion set(associated to S) : $S_{/R} := \{\overline{x} | x \in S\}$
- The **equivalence class** of an equivalence relation on A from a partition of A is a set of elements considered equivalent under the equivalence relation .

4.2.2 Order relations :

• R must be reflexive , anti-symmetric and transitive
types of order relations :
Partial : if there exist some elements from the domain that there is no relation between them .
Total : $\succeq$ if all the elements have a relation between them .
Some properties :

- maximal : there doesn't exist an element $b \in A$, $b \neq a \ and \ b \succeq a$
- minimal : there doesn't exist an element $b \in A$, $b \neq a \ and \ a \succeq b$
- The last element : $a \in A$ the least element of A if $a \preceq b$, $\forall b \in A$
- The Greatest element : $a \in A$ the greatest element of A if $a \succeq b$, $\forall b \in A$
- Upper bound : if $\exists s \in S, a \preceq s$, $\forall a \in A$ then s is the upper bound $(A \subset S)$
- Lower bound : if $\exists s \in S, a \succeq s$, $\forall a \in A$ then s is the lower bound

Chapter 03: Algebraic structures

5 Binary operations :

Let be a binary operation on S it is a map :

$$: S \times S \longrightarrow S$$

$$(x, y) \mapsto (x, y) = xy$$

5.1 Some properties of Binary operations :

- **Commutative :** $\forall x, y \in S \; ; \; xy = yx$
- **Associative :** $\forall x, y, z \in S \; ; \; x(\, yz\,) = (\, xy\,)z$
- **Neutral element :** $\exists e \in S \; , \; \forall x \in S \; ; \; xe = ex = x$ "e is unique"
- **Invertible :** $\exists x' \in S, \forall x \in S \; ; \; x'x = xx' = e$; x' is the inverse of x by and it is denoted by :
  x^{-1} if is multiplicative (has the properties of multiplication)
  $-x$ if is additive (has the properties of addition)

Note :

- if is a binary operation that is associative and have a neutral element then every inverse element is unique .
- if x and y invertible under associative binary operation on S .

Then xy is also invertible and we have $(xy)^{-1} \; = \; y^{-1}x^{-1}$.
- is multiplicative then :

$$x^n = \begin{cases} x \times x \times x \times ... \times x & if n > 0 \\ e & if n = 0 \\ x^{-1} \times x^{-1} \times x^{-1} \times ... \times x^{-1} & if n < 0 \end{cases}$$

- is additive then :

$$nx = \begin{cases} x + x + x + ... + x & if n > 0 \\ e & if n = 0 \\ (-x) + (-x) + (-x) + ... + (-x) & if n < 0 \end{cases}$$

6 Groups : (G,)

Definition :

- is associative .
- (G,) has a neutral element .($\Rightarrow$ non empty)
- every element of G has an inverse .

6.1 Abelian group (Commutative group) :

It is a group such that is commutative $\forall g_1, g_2 \in G$; $g_1 g_2 = g_2 g_1$

6.2 Subgroup :

(G,) is a group , H is a subset of G ; we say that H is a subgroup of G if (H,) is a group and we denote $H \leq G$.

$$multiplicative \quad : \quad (H \leq G) \Leftrightarrow (e_G \in H \wedge \ \forall x, y \in H \, , xy^{-1} \in H)$$

$$additive \quad : \quad (H \leq G) \Leftrightarrow (e_G \in H \wedge \ \forall x, y \in H \, , x(-y) \in H)$$

Note : all subgroups of $\mathbb{Z}$ are from the type k$\mathbb{Z}$; k $\in \mathbb{N}_0$.

6.3 Order of a group : (Cardinality) $|G|$

- $|G| \leq 1$
- if $|G| = 1 \Leftrightarrow |G| = \{e_G\}$
- $|G| < \infty$ (infinite otherwise)

La group theorem :

G is a finite group then : $H \leq G \Rightarrow |H| \ | \ |G|$

6.4 Homomorphism & isomorphism of a group :

Let (G,) and (G′,) be groups , a group homomorphism from (G,) to (G′,) is a map :
$f : G \longrightarrow G'$ such that $\forall u, v \in G$; $f(uv) = f(u)f(v)$.
a group homomorphism $f : (G,) \longrightarrow (G',)$ is called :

1. group **monomorphism** if f is injective .
2. group **epimorphism** if f is surjective .
3. group **isomorphism** if f is bijective .
4. group **endomorphism** if (G,) = (G′,) .
5. group **automorphism** if f is bijective and (G,) = (G′,) .

Note : we say that two groups(G and G′) are isomorphic if there is an isomorphism from G to G′ (G≈G′) .

Some properties :

let $f : (G_1,_1) \longrightarrow (G_2,_2)$ be a group homomorphism ;

- $f(e_{G_1}) = e_{G_2}$
- $f(x^{-1}) = [f(x)]^{-1}, \forall x \in G_1$
- $f(x^n) = [f(x)]^n, \forall x \in G_1, \forall n \in \mathbb{Z}$
- H_1 *is a subgroup of* $G_1 \Rightarrow f(H_1)$ *is a subgroup of* G_2
- H_2 *is a subgroup of* $G_2 \Rightarrow f^{-1}(H_2)$ *is a subgroup of* G_1

6.5 Image and Kernel :

Image : $f(G_1) = Im_f = \{f(x) \mid x \in G_1\} \subset G_2$ "Im_f is a subgroup of G_2"
Kernel : $f^{-1}(\{e_{G_2}\}) = Ker_f = \{x \in G_1 | f(x) = e_{G_1}\} \subset G_1$ "Ker_f is a subgroup of G_1"
Note : f is injective $\Leftrightarrow$ $Ker_f = \{e_{G_1}\}$; f is surjective $\Leftrightarrow$ $Im_f = G_2$

6.6 Cyclic groups :

a group G IS called **cyclic** if $\exists g \in G, \forall g \in G$, we can express it by the (power/sum) of g :
• multiplicative : $G = \{g^n \mid n \in \mathbb{Z}\}$
• additive : $G = \{ng \mid n \in \mathbb{Z}\}$
g is called the generator of G ¡g¿(it can have more then one)
Notes : $G = \{e, g, g^2, ..., g^{n-1}\}; n = |G|$

$$G \text{ is } finite \Rightarrow g^i = g^j \Leftrightarrow i = j$$

$$G \text{ is } infinite \Rightarrow g^i = g^j \Leftrightarrow n|(i-j)$$

every cyclic group is abelian .

6.7 Order of element :

$a \in G$, the order of a is the order of the group generated by a , $< a >= \{a^n \mid n \in \mathbb{Z}\}$, (ord(a)) and it is the smallest positive integer ($\neq 0$) m such that $a^m = e$

In finite group :

- G finite cyclic group $\Rightarrow ord(a) \mid |G|$.
- $ord(a) = n$; $a \in G$; $\left\langle a^k \right\rangle = \left\langle a^{gcd(a,k)} \right\rangle$ and $ord(a^k) = \frac{n}{gcd(n,k)}; k \in \mathbb{Z}$.
- subgroup of cyclic group is cyclic .
- group of a prime order cyclic group .

6.8 the group of integer module n : $n \in \mathbb{Z}, \sim$ *is an equivalence relation in* $\mathbb{Z}$

$a \sim b \Leftrightarrow a \equiv b \; mood \; n \; ; \; (a - b = kn), k \in \mathbb{Z} \; ; \; (a - b \in n\mathbb{Z})$.
$\overline{a} = \{x \in \mathbb{Z} \mid x \sim a\} = \{x \in \mathbb{Z} \mid x \equiv a \; mood \; n\} = \{x \in \mathbb{Z} \mid x - a \in n\mathbb{Z}\}$.
$\overline{a} = \{x \in n\mathbb{Z} + a\} = n\mathbb{Z} + a$.

- the set of integers mood n denoted by $\mathbb{Z}_n$ or $\mathbb{Z}/_{n\mathbb{Z}}$ is denoted by :

$$\mathbb{Z}_n = \mathbb{Z}/_{n\mathbb{Z}} = \{\overline{a} \mid a \in \{0, 1, ..., n-1\}\} \; ; \; |\mathbb{Z}_n| = n$$

- we can define addition and multiplication operations on $\mathbb{Z}_n$ denoted by :

$$\overline{a} + \overline{b} = \overline{a + b} \; ; \; \overline{a} \times \overline{b} = \overline{a \times b}$$

Theorem : $(\mathbb{Z}_n; +)$ is an abelian group
• every cyclic group of order n is isomorphic to $\mathbb{Z}_n$
• every infinite cyclic group is isomorphic to $\mathbb{Z}$

6.9 External product of a group : $(G_1; \star_1); (G_2; \star_2)$

$G_1 \times G_2 = \{(g_1, g_2 \mid g_1 \in G_1 \wedge g_2 \in G_2\}$

$$: (G_1 \times G_2) \times (G_1 \times G_2) \longrightarrow (G_1 \times G_2)$$

$$((g_1, g_2), (g_1', g_2')) \mapsto ((g_1 \star_1 g_1'), (g_2 \star_2 g_2'))$$

$(G_1 \times G_2,)$ is a group .

- G_1, G_2 are commutative $\Rightarrow$ (G_1, G_2) is commutative .
- G_1, G_2 finite $\Rightarrow$ $G_1 \times G_2$ finite $\wedge |G_1 \times G_2| = |G_1| \cdot |G_2|$.
- $g_1 \in G_1$, $g_2 \in G_2$ have finite order then (g_1, g_2) has finite order

$$ord((g_1, g_2)) = lcm(ord(g_1), ord(g_2))$$

7 Rings :$(R, +, \cdot)$

Definition :

- (R,+) is an abelian group .
- $\cdot$ is associative .
- $\cdot$ is distributive on + .

Commutative ring : $a \cdot b = b \cdot a, \forall a, b \in R$
Ring with unity : $1_R \in R : a \cdot 1_R = a \cdot 1_R = a, \forall a \in R$

7.1 Calculating rules of a ring : $\forall a, b \in R$

- $0_R \cdot a \;=\; a \cdot 0_R \;=\; 0_R$
- $(-a) \cdot b \;=\; a \cdot (-b) \;=\; -(a \cdot b)$
- $(-a)(-b) \;=\; a \cdot b$
- R ring with unity $\Leftrightarrow -a \;=\; -1_R \cdot a$; $\forall a \in R$

7.2 Special elements in a ring :

• R is a ring with unity That a is unity (invertible) if a has a multiplicative inverse
($if\ \exists b \in R, a \cdot b \;=\; b \cdot a \;=\; 1_R$)
the set of invertible elements is denoted by $R^\times$ or $U(R)$
•**Zero divisors :** Let $a \neq 0_R$ be an element of R , a is zero divisor if $\exists b \neq 0_R$; $a \cdot b = b \cdot a = 0_R$.
•**Nilpotent and Idempotent :** $a \in R$
nilpotent $\Rightarrow a^k = 0_R$, $k \in \mathbb{N}$.
idempotent $\Rightarrow a^2 = a$.

7.3 Integral domain :

a commutative ring with unity is an integral domain iff it has no zero divisors
($a \cdot b \;=\; 0 \Rightarrow a \;=\; 0 \vee b \;=\; 0$).
• If R is an integral domain and a , b , c $\in R$ with $a \neq 0$, $a \cdot b \;=\; a \cdot c$ then b = c ."in groups we can do this because of inverses but here it is not the case"

7.4 Subring : $(R, +, \cdot)$ a ring , $S \neq \emptyset$ is a subring of R

If $(S, +, \cdot)$ is a ring ,then S is a subring of R .
Subring test : S is a subring $\Leftrightarrow (0_R \in S \;\wedge\; a - b \in S \;\wedge\; a \cdot b \in S$, $\forall a, b \in S)$

7.5 Ring homomorphism : $\phi : R \Longrightarrow R'(R, R'$ *is rings* $)$ *is a ring homomorphism*

- $\phi(a +_R b) \;=\; \phi(a) +_{R'} \phi(b) \wedge \phi(a \times_R b) \;=\; \phi(a) \times_{R'} \phi(b)$
- $\phi(0_R) \;=\; 0_{R'}$
- $\phi(-a) \;=\; -\phi(a)$
- $\phi(a - b) \;=\; \phi(a) - \phi(b)$

Theorem :

- ker_ϕ is a subring of R .
- ϕ is injective $\Leftrightarrow ker_\phi = \{0_R\}$.
- If S is a (commutative) subring of R then $\phi(S)$ is a (commutative) subring of R' .

7.6 Ideals :

I a subring of R and it is an ideal $\Rightarrow\ \forall r \in R\ \wedge\ \forall a \in I, ra \in I\ \wedge\ ar \in I$.
$\{0_R\} \in I \subset R$ is an ideal : $a, b \in I$, $a - b \in I$; $\forall r \in R\ \wedge\ \forall a \in I$, $ra \in I\ \wedge\ ar \in I$.

7.7 Characteristic of a ring : R is a ring

$\exists n \in \mathbb{N}$; $n \cdot a = 0_R$, $\forall a \in R$, the smallest element n is called the characteristic of R , char(R)
char(R) = 0 if it doesn't exist .
• R ring with unity :

- $n \cdot 1_R \neq 0_R$, $\forall n \in \mathbb{N}$, *then* $char(R) = 0$.
- $n \cdot 1_R = 0_R$ *for some* $n \in \mathbb{N}$ *then* $char(R) = n$.

• The characteristic of integral domain is either 0 or a prim number .

8 Fields :(F,+,$\times$)

Definition :

- (F,+) is an abelian group .
- $(F - \{0_F\}, \times)$ is a group .
- $\times$ is distributive on + .

8.1 Subfield : L is a subfield of F "subfield test"

L is a subfield of F $\Leftrightarrow (\forall a, b \in L\ ,\ a + b \in L\ ,\ a \times b \in L) \wedge \big(\forall x \in L\ ,\ -x \in L\ \wedge\ \forall x \in L - \{0_F\}\ ,\ x^{-1} \in L\big) \wedge 1_F \in L$

9 Arithmetic in $\mathbb{Z}$: $r, a, b, n, q, p \in \mathbb{Z}\ ;\ n > 0$

a congruent to b modulo n $\Leftrightarrow a \equiv b\ mood\ n (n|b - a)$.
r is the reminder when $n|r$ then $a \equiv r\ mood\ n$.
$a \equiv a[n]$; $a \equiv b[n] \Leftrightarrow a \equiv b[n]$; $a \equiv b[n] \wedge b \equiv c[n] \Rightarrow a \equiv c[n]$
$a \equiv b[n] \wedge c \equiv d[n] \Rightarrow a + c \equiv b + d[n]$; $a \equiv b[n] \wedge c \equiv d[n] \Rightarrow a \cdot c \equiv b \cdot d[n]$
$a \equiv b[n] \Rightarrow a^j \equiv b^j[n]$; $\forall j \geq 1$
Fermat little theorem : p is prim , $q \in \mathbb{Z}, qp$ then $q^{p-1} \equiv 1\ mood\ p$.
Euler's theorem : $gcd(a, n) = 1$ then $a^{\phi(n)} \equiv 1\ mood\ n$.
Chinese remainder theorem : $n_i \in \mathbb{N}n\{1\}, a_i \in \mathbb{Z}\ ;\ i = \{0, 1, ..., k\}$

$$\begin{cases} x \equiv a_1 moodn_1 \\ \vdots\vdots \\ x \equiv a_k moodn_k \end{cases}$$

the unique solution x is given by : $N = n_1 \times n_2 \times ... \times n_k$
$N_i = \frac{N}{n_i}$ and $N_i y_i \equiv 1\ mood\ n_i$, $\forall i = \{1, 2, ..., k\}$ $x = a_1 N_1 y_1 + ... + a_k N_k y_k\ mood\ N$.

Chapter 04: Polynomials and rational fractions "$\mathbb{K}$ is a commutative field "

10 Polynomials :

10.1 Generalities :

- a polynomial P is one variable with coefficients in $\mathbb{K}$; $n \in \mathbb{N}, \forall i \in \{\overline{0,n}\}; a \in \mathbb{K}$; it expression is $P(X) = a_n X^n + a_{n-1} X^{n-1} + ... + a_1 X + a_0 = \sum_{i=0}^{n} a_i X^i$ a_i is the coefficient of $P(X)$.
- $\mathbb{K}[X]$ is the set of all polynomials .
- the zero polynomial $0_{\mathbb{K}[X]}$ is when , $\forall i$, $a_i = 0$, $a_i X^i$ is a monomial .
- the degree of a polynomial $deg(P) = max\{i \mid a_i \neq 0_{\mathbb{K}}\}$; $deg(0_{\mathbb{K}}) = -\infty$.
- the polynomial is said to be monic if $a_n = 1_{\mathbb{K}}$ (the highest degree's polynomial) .
- $\mathbb{K}_n[X] := \{P(X) \in \mathbb{K}[X] \mid deg(P) \leq n\}$.

10.2 Operations on polynomials : $P(X) = \sum_{i=0}^{n} a_i X^i$, $Q(X) = \sum_{i=0}^{n} b_i X^i$, $\lambda \in \mathbb{K}$

10.2.1 Addition :

$(P+Q)(X) = \sum_{i=0}^{n} (a_i + b_i) X^i$.

10.2.2 Product :

$(PQ)(X) = \sum_{i=0}^{n} c_i X^i$; $c_i = \sum_{k+j=i} a_k b_j$
$(\lambda P)(X) = \sum_{i=0}^{n} \lambda a_i X^i$; $if P = Q \Rightarrow a_i = b_i$, $\forall i$

10.3 Some properties :

- $0_{\mathbb{K}[X]} + P = P$; $1_{\mathbb{K}} \times P = P$; $P \times (Q+R) = PQ + PR$; $PQ = QP$
- $P + (Q+R) = (P+Q) + R$; $P \times (Q \times R) = (P \times Q) \times R$; $P + Q = Q + P$
- $deg(P \times Q) = deg(P) + deg(Q)$; $deg(P+Q) \leq max\{deg(P); deg(Q)\}$

Theorem :
• $\mathbb{K}[X]$ is a commutative ring , an integral domain
• $(\mathbb{K}[X])^{\times} = \mathbb{K}[X] - \{0_{\mathbb{K}}\}$

10.4 Arithmetics of polynomials : $A, B, C, P, Q, R, U, V \in \mathbb{K}[X]$, $\lambda, \mu \in \mathbb{K}$

10.4.1 Euclidean division :

$B|A$ (B divides A) id $A = B \times Q$ (A multiple of B) .
if $A|B \ \wedge B|C$ then $A|C$; $A|B \wedge B|A \ \Rightarrow A = \lambda B$; $C|A \ \wedge \ C|B \Rightarrow C|A\mu + B\lambda$
euclidean division : $A = BQ + R \wedge deg(R) < deg(B)$; A is the dividend , B is divisor , Q is the quotient , R is the reminder. if $R = 0$ then $B|A$

10.4.2 GCD of polynomial :

is a unique monic polynomial of highest degree such that $GCD(A, B)|A \ \wedge \ GCD(A, B)|B$.
• if $A|B \ \wedge \ A \neq 0_{\mathbb{K}[X]}$ then $GCD(A, B) = \frac{1}{\lambda}A$ (λ is the dominant coefficient of A) .
• $GCB(\lambda A, \mu B) = GCD(A, B)$.
• $A = BQ + R \Rightarrow GCD(A, B) = GCD(B, R)$; $GCD(A, 0) = A$.

10.4.3 Euclidean algorithem for polynomials :

$A = BQ_1 + R_1 \ \Rightarrow \ GCD(A, B) = GCD(B, R_1)$
$B = R_1Q_2 + R_2 \ \Rightarrow \ GCD(B, R_1) = GCD(R_1, R_2)$
$\vdots \qquad \vdots \qquad\qquad \vdots$
$R_{k-2} = R_{k_1}Q_k + R_k \ \Rightarrow \ GCD(R_{k-2}, R_{k-1}) = GCD(R_{k-1}, R_k)$
$R_{k-1} = R_kQ_{k+1} + 0_{\mathbb{K}[X]} \ \Rightarrow \ GCD(R_{k-1}, R_k) = \frac{1}{\lambda}R_k$.
thus $GCD(A, B) = frec1kR_k$ (we stop the algorithm when the reminder is $0_{\mathbb{K}[X]}$) .

10.4.4 Bezout theorem : let $A, B \in (\mathbb{K}[X])^\times$, $\exists U, V \in \mathbb{K}[X]$

$$AU + BV = GCD(A, B)$$

thus if A and B are relatively prim (coprim) : $AU + BV = 1$.
Gauss lemma : If $A|BC \ \wedge \ GCD(A, B) = 1 \Rightarrow A|C$
• if $C|A \wedge C|B$ then $C|GCD(A, B)$.

10.5 Roots of a polynomial and Fractionation : $let\ P \in \mathbb{K}[X]$

for any $x \in \mathbb{K}$:

$$P : \mathbb{K} \longrightarrow \mathbb{K}$$
$$x \mapsto P(x)$$

is a polynomial function associated to the polynomial P .

10.5.1 Root of polynomial :

α is a root of P(x) ; $P(\alpha) = 0_{\mathbb{K}}$; $P(X) = Q(X)(X - \alpha)$.

10.5.2 multiplicity of a root of a polynomial :

α is said to be a root of multiplicity k of P if $(x-\alpha)^k | P \ \wedge \ (x-\alpha)^{k+1} P$
• if $k=1 \Rightarrow$ it is a simple root ; $k=2 \Rightarrow$ it is a double root ; $k=3$ it is a triple root ; ...
• α is a root of multiplicity k of $P \Leftrightarrow \ \exists Q \in \mathbb{K}[X] \ : \ P(X) = (x-\alpha)^k Q(X); Q(\alpha) \neq 0_{\mathbb{K}} \ \Leftrightarrow$
$P(\alpha) = P'(\alpha) = ... = P^{(k-1)}(\alpha) = 0_{\mathbb{K}} \ \wedge \ P^{(k)}(\alpha) \neq 0_{\mathbb{K}}$.
Corollary : $P \in \mathbb{K}[X]$; $\alpha_1, \alpha_2, ..., \alpha_n$ be roots of P of multiplicity $k_1, k_2, ..., k_n$ respectively .

$$P(X) = (X-\alpha_1)^{k_1} \times (X-\alpha_2)^{k_2} \times ...(X-\alpha_n)^{k_n} Q(X) \ ; \ Q(\alpha_i) = \neq 0_{\mathbb{K}} \ ; \ \forall i \in \{\overline{1,r}\}$$

.

10.6 Fundamental theorem of algebra :

every polynomial of degree $n \geq 1$ has n complex roots (with their multiplicity) and in general it has at most n roots in $\mathbb{K}$. ($0_{\mathbb{K}[X]}$ has roots more then it's degree)

10.7 Irreducible polynomials :(non constant polynomials)

• if it can not be factored into a product of two or more polynomials with coefficients in $\mathbb{K}$ (if it is not irreducible than it is reducible) .
• it's devisers are constants or λP ; $\lambda \in \mathbb{K}^*$.
• if $P \in \mathbb{K}[X] \wedge deg(P) is 2 or 3$ then P is said to be irreducible if it has no roots in $\mathbb{K}$.
• irreducible polynomials in $\mathbb{C}[X]$ are : $P(X) = a + bX$, $a, b \in \mathbb{C}$.
• irreducible polynomials in $\mathbb{R}[X]$ are : $P(X) = (a + bX \ , \ a, b \in \mathbb{R} \vee aX^2 + bX + c \ , \ a, b, c \in \mathbb{R}) \wedge (b^2 - 4ac < 0)$.

10.8 Factorization of polynomials in $\mathbb{C}[X]$; $\mathbb{R}[X]$:

• let $P(X) \in \mathbb{C}[X]$; $P(X) = C(X-r_1)^{k_1}(X-r_2)^{k_2}...(X-r_p)^{k_p} = C\prod_{i=0}^{p}(X-r_i)^{k_i}$; $r_i \mathbb{C}, k_i \in \mathbb{N}, \forall i \in \{\overline{1,p}\}$; $n = \sum_{i=1}^{p}$. (C is the leading coefficient of P)
• let $P(X) \in \mathbb{R}[X]$; $P(X) = C(X-r_1)^{k_1}(X-r_2)^{k_2}...(X-r_p)^{k_p}(X^2 + a_{p+1}X + b_{p+1})^{k_{p+1}}...(X^2 + a_l X + b_l)^{k_l} = C\prod_{i=1}^{p}(X-r_i)^{k_i} \times \prod_{i=p+1}^{l}(X^2 + a_i X + b_i)^{k_i}$ $a_i, b_i, r_i \in \mathbb{R}$; $k_i \in \mathbb{N}$, $\forall i$; $a_i^2 - 4b_i < 0$; $\sum_{i=1}^{p} k_i + 2\sum_{i=p+1}^{l} k_i = n$.
• $\alpha \in \mathbb{C}$ is a root of P with multiplicity r , $\overline{\alpha}$ is also a root of P of multiplicity r .
• $(X-\alpha)(X-\overline{\alpha}) = X^2 - 2Re(\alpha) + |\alpha|^2 \in \mathbb{R}[X]$; $\alpha, \overline{\alpha} \in \mathbb{C}$.

Note : for rational fractions we did't have time to do them in class so they are in analysis 2 indefinite integrals chapter ;) .